IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of	:	
Yuichi FUTA et al.	:	
Serial No. NEW	:	**Attn: APPLICATION BRANCH**
Filed April 13, 2004	:	Attorney Docket No. 2004_0582A
APPARATUS AUTHENTICATION SYSTEM, SERVER APPARATUS, AND CLIENT APPARATUS	:	

CLAIM OF PRIORITY UNDER 35 USC 119

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

THE COMMISSIONER IS AUTHORIZED TO CHARGE ANY DEFICIENCY IN THE FEES FOR THIS PAPER TO DEPOSIT ACCOUNT NO. 23-0975

Sir:

Applicants in the above-entitled application hereby claim the date of priority under the International Convention of Japanese Patent Application No. 2003-109264, filed April 14, 2003, as acknowledged in the Declaration of this application.

A certified copy of said Japanese Patent Application is submitted herewith.

Respectfully submitted,

Yuichi FUTA et al.

By _____
Jeffrey R. Filipek
Registration No. 41,471
Attorney for Applicants

JRF/fs
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
April 13, 2004

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　４月１４日

出願番号
Application Number: 特願２００３－１０９２６４

[ST. 10/C]: ［ＪＰ２００３－１０９２６４］

出願人
Applicant(s): 松下電器産業株式会社

２００４年　２月１０日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００４－３００８２９３

【書類名】　特許願
【整理番号】　2022550157
【提出日】　平成15年 4月14日
【あて先】　特許庁長官　殿
【国際特許分類】　G06F 12/14
【発明者】
【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
【氏名】　布田　裕一
【発明者】
【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
【氏名】　松崎　なつめ
【発明者】
【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
【氏名】　山内　弘貴
【発明者】
【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
【氏名】　太田　雄策
【発明者】
【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
【氏名】　臼木　直司
【発明者】
【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
【氏名】　綾木　靖

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　森岡　芳宏

【特許出願人】

【識別番号】　000005821

【氏名又は名称】　松下電器産業株式会社

【代理人】

【識別番号】　100090446

【弁理士】

【氏名又は名称】　中島　司朗

【手数料の表示】

【予納台帳番号】　014823

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9003742

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　機器認証システム、機器認証装置、機器認証方法及び記録媒体

【特許請求の範囲】

【請求項１】第１のネットワークに接続しているサーバにより第２のネットワークに接続している機器を認証する機器認証システムであって、

前記サーバは、チャレンジデータを作成し、前記機器へ送信するチャレンジ送信手段と、

署名データを受信する署名受信手段と、

前記署名データが、前記チャレンジデータと前記サーバに予め設定されている第１のパスワードデータに基づく第１の署名対象データに対する正しい署名であるか否かを検証する署名検証手段を備え、

前記機器は、前記チャレンジデータを受信するチャレンジ受信手段と、

前記チャレンジデータと、前記機器に予め設定されている第２のパスワードデータに基づく第２の署名対象データを作成する署名対象データ作成手段と、

前記第２の署名対象データに対する前記署名データを作成する署名作成手段と、

前記署名データを送信する署名送信手段を備える

ことを特徴とする機器認証システム。

【請求項２】前記第２のパスワードデータは、外部から入力されることを特徴とする請求項１記載の機器認証システム。

【請求項３】前記機器は、さらに外部より入力された第３のパスワードデータを前記第２のパスワードデータに登録するパスワード登録手段を備えることを特徴とする請求項１記載の機器認証システム。

【請求項４】前記機器は、さらにネットワークを介して前記第３のパスワードデータを受信するパスワード受信手段と、

前記第３のパスワードデータが送信されたパスワード送信元が前記第２のネットワークに接続しているか否かを判定するパスワード送信元判定手段を備え、

前記パスワード登録手段は、前記パスワード送信元が前記第２のネットワークに接続していると判定された場合のみに、前記第３のパスワードデータを前記第

２のパスワードデータに登録する

ことを特徴とする請求項３記載の機器認証システム。

【請求項５】前記機器は、さらに前記第３のパスワードデータの長さを計測し、前記第３のパスワードデータの長さが予め与えられた値以上であるか否かを判定するデータ長判定部を備え、

前記パスワード登録手段は、前記第３のパスワードデータの長さが予め与えられた値以上である場合に、前記第３のパスワードデータを前記第２のパスワードデータに登録する

ことを特徴とする請求項３記載の機器認証システム。

【請求項６】前記サーバは、さらに前記第２のネットワークが前記第１のネットワークと同一であることを判定するネットワーク判定手段を備え、

前記署名検証手段は、前記判定が肯定的である場合、前記署名データが前記チャレンジデータと前記サーバに予め設定されている第４のパスワードデータに基づく第３の署名対象データに対する正しい署名であるか否かを検証し、否定的である場合、前記前記署名データが前記チャレンジデータと前記サーバに予め設定されている第５のパスワードデータに基づく第４の署名対象データに対する正しい署名であるか否かを検証する

ことを特徴とする請求項１から請求項４のいずれか１項に記載の機器認証システム。

【請求項７】前記署名生成手段及び前記署名検証手段で使用する署名方法は公開鍵署名方法であることを特徴とする請求項１から請求項６のいずれか１項に記載の機器認証システム。

【請求項８】前記署名生成手段及び前記署名検証手段で使用する署名方法は鍵付ハッシュ関数を利用することを特徴とする請求項１から請求項６のいずれか１項に記載の機器認証システム。

【請求項９】機器を認証する機器認証装置であって、

チャレンジデータを作成し、前記機器へ送信するチャレンジ送信部と、

署名データを受信する署名受信部と、

前記署名データが、前記チャレンジデータと予め設定されている第１のパスワ

ードデータに基づく第１の署名対象データに対する正しい署名であるか否かを検証する署名検証手段を備える

ことを特徴とする機器認証装置。

【請求項１０】さらに前記機器が接続している第２のネットワークが前記機器認証装置が接続している第１のネットワークと同一であることを判定するネットワーク判定手段を備え、

前記署名検証手段は、前記判定が肯定的である場合、前記前記署名データが前記チャレンジデータと前記サーバに予め設定されている第４のパスワードデータに基づく第３の署名対象データに対する正しい署名であるか否かを検証し、否定的である場合、前記前記署名データが前記チャレンジデータと前記サーバに予め設定されている第５のパスワードデータに基づく第４の署名対象データに対する正しい署名であるか否かを検証する

ことを特徴とする請求項９記載の機器認証装置。

【請求項１１】第１のネットワークに接続しているサーバにより第２のネットワークに接続している機器を認証する機器認証方法であって、

前記サーバにより、チャレンジデータを作成し、前記機器へ送信するチャレンジ送信ステップと、

前記機器により、前記チャレンジデータを受信するチャレンジ受信ステップと、

前記機器により、前記チャレンジデータと、前記機器に予め設定されている第２のパスワードデータに基づく第２の署名対象データを作成する署名対象データ作成ステップと、

前記機器により、前記第２の署名対象データに対する署名データを作成する署名作成ステップと、

前記機器により、前記署名データを送信する署名送信ステップと、

前記サーバにより、署名データを受信する署名受信ステップと、

前記サーバにより、前記署名データが、前記チャレンジデータと前記サーバに予め設定されている第１のパスワードデータに基づく第１の署名対象データに対する正しい署名であるか否かを検証する署名検証ステップを含む

ことを特徴とする機器認証方法。

【請求項１２】さらに、前記機器により、外部より入力された第３のパスワードデータを前記第２のパスワードデータに登録するパスワード登録ステップを含むことを特徴とする請求項１１記載の機器認証方法。

【請求項１３】さらに、前記機器により、ネットワークを介して前記第３のパスワードデータを受信するパスワード受信ステップと、

前記機器により、前記第３のパスワードデータが送信されたパスワード送信元が前記第２のネットワークに接続しているか否かを判定するパスワード送信元判定ステップを含み、

前記パスワード登録ステップは、前記機器により、前記パスワード送信元が前記第２のネットワークに接続していると判定された場合のみに、前記第３のパスワードデータを前記第２のパスワードデータに登録する

ことを特徴とする請求項１１記載の機器認証方法。

【請求項１４】さらに、前記サーバにより、前記第２のネットワークが前記第１のネットワークと同一であることを判定するネットワーク判定ステップを含み

、

前記署名検証ステップは、前記サーバにより、前記判定が肯定的である場合、前記前記署名データが前記チャレンジデータと前記サーバに予め設定されている第４のパスワードデータに基づく第３の署名対象データに対する正しい署名であるか否かを検証し、否定的である場合、前記前記署名データが前記チャレンジデータと前記サーバに予め設定されている第５のパスワードデータに基づく第４の署名対象データに対する正しい署名であるか否かを検証する

ことを特徴とする請求項１１から請求項１３のいずれか１項に記載の機器認証方法。

【請求項１５】第１のネットワークに接続しているサーバにより第２のネットワークに接続している機器を認証する処理をコンピュータに実行させるプログラムを記録したコンピュータ読取可能な記録媒体であって、

前記サーバにより、チャレンジデータを作成し、前記機器へ送信するチャレンジ送信ステップと、

前記機器により、前記チャレンジデータを受信するチャレンジ受信ステップと、

前記機器により、前記チャレンジデータと、前記機器に予め設定されている第２のパスワードデータに基づく第２の署名対象データを作成する署名対象データ作成ステップと、

前記機器により、前記第２の署名対象データに対する署名データを作成する署名作成ステップと、

前記機器により、前記署名データを送信する署名送信ステップと、

前記サーバにより、署名データを受信する署名受信ステップと、

前記サーバにより、前記署名データが、前記チャレンジデータと前記サーバに予め設定されている第１のパスワードデータに基づく第１の署名対象連結データに対する正しい署名であるか否かを検証する署名検証ステップと

をコンピュータに実行させることを特徴とするプログラムを記録したコンピュータ読取可能な記録媒体。

【請求項１６】さらに、前記機器により、外部より入力された第３のパスワードデータを前記第２のパスワードデータに登録するパスワード登録ステップ

をコンピュータに実行させることを特徴とするプログラムを記録した請求項１５記載のコンピュータ読取可能な記録媒体。

【請求項１７】さらに、前記機器により、ネットワークを介して前記第３のパスワードデータを受信するパスワード受信ステップと、

前記機器により、前記第３のパスワードデータが送信されたパスワード送信元が前記第２のネットワークに接続しているか否かを判定するパスワード送信元判定ステップをコンピュータに実行させ、

前記パスワード登録ステップは、前記機器により、前記パスワード送信元が前記第２のネットワークに接続していると判定された場合のみに、前記第３のパスワードデータを前記第２のパスワードデータに登録する

ことを特徴とするプログラムを記録した請求項１６記載のコンピュータ読取可能な記録媒体。

【請求項１８】さらに、前記サーバにより、前記第２のネットワークが前記第

１のネットワークと同一であることを判定するネットワーク判定ステップをコンピュータに実行させ、

前記署名検証ステップは、前記サーバにより、前記判定が肯定的である場合、前記前記署名データが前記チャレンジデータと前記サーバに予め設定されている第４のパスワードデータに基づく第３の署名対象データに対する正しい署名であるか否かを検証し、否定的である場合、前記前記署名データが前記チャレンジデータと前記サーバに予め設定されている第５のパスワードデータに基づく第４の署名対象データに対する正しい署名であるか否かを検証する

ことを特徴とするプログラムを記録した請求項１５から請求項１７のいずれか１項に記載のコンピュータ読取可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、機器認証システム、機器認証装置、機器認証方法及び記録媒体に関し、特にパスワード認証を機器認証に組み合わせることによりコンテンツの著作権保護を図りつつ、実装上の負荷を軽減する技術に関する。

【０００２】

【従来の技術】

近年、音楽や映像、ゲームなどデジタルコンテンツはインターネットやデジタル放送および、パッケージメディアによる流通により容易に取得が可能となってきている。

このようなシステムでは、通常、コンテンツの著作権を保護するために、コンテンツは暗号化され、それを獲得する権利のある機器だけが復号できるようになっている。例えば、インターネットを用いたデジタルコンテンツの配布では、配布元であるサーバと、コンテンツを利用するクライアント機器の間で認証が行われ、サーバは予め登録されたクライアント機器であることを確認後、コンテンツをそのクライアント機器だけが有する鍵を用いて暗号化して配布する。

【０００３】

以下に、サーバとクライアント機器間の認証方法の一例として、公開鍵暗号を

用いた相手認証方法を示す（例えば、非特許文献１参照）。

第１の機器が第２の機器にチャレンジデータとして乱数データを送信し、続いて、第２の機器がその乱数データに対して自分の秘密鍵で暗号化（電子署名など）して第１の機器にレスポンスデータを返信し、最後に、返信されてきた暗号文（あるいは、署名文）に対して、第１の機器が第２の機器の公開鍵を用いて検証するというものがある。一般に、このような公開鍵暗号を用いた認証においては、公開鍵そのものが有効であることが前提となる。

【０００４】

このために、認証局と呼ばれる機関から、各機器に対応する正しい公開鍵であることを示す（公開鍵に対する「お墨付き」となる）「公開鍵証明書」が発行されることが一般的である。公開鍵証明書は、機器の識別名や有効期限と公開鍵を結合したデータに認証局の電子署名が付与されたものであり、これを受け取った機器は、その電子署名の正しさを確認し、さらに通信機器の識別名や現在の時間からその公開鍵証明書の記載内容を確認した上で、公開鍵の正しさを確認するものである。さらに、発行された公開鍵証明書のうち、不正を働いた機器、あるいは秘密鍵が盗まれた機器の公開鍵証明書については、それらが無効化されていることを他の機器に知らせるために、無効化した公開鍵証明書を特定する情報の一覧に対して認証局の電子署名が付与された公開鍵証明書無効化リスト（Ｃｅｒｔｉｆｉｃａｔｅ　Ｒｅｖｏｃａｔｉｏｎ　Ｌｉｓｔ：以下、ＣＲＬ）として発行される（例えば、非特許文献２参照）。

【０００５】

このように、相手機器の公開鍵を用いてその相手機器を認証する際には、その相手機器から公開鍵証明書を入手し、入手した公開鍵証明書がＣＲＬに登録されたもの（無効化されたもの）でないことを確認する。

一方、高速シリアルバス規格の１つのＩＥＥＥ１３９４を介して配信されるデジタルコンテンツの保護規格として、ＤＴＣＰ（Ｄｉｇｉｔａｌ　Ｔｒａｎｓｍｉｓｓｉｏｎ　Ｃｏｎｔｅｎｔ　Ｐｒｏｔｅｃｔｉｏｎ）と呼ばれる規格がある（例えば、非特許文献３参照）。

【０００６】

ＤＴＣＰでは、ＤＴＬＡ（Ｄｉｇｉｔａｌ　Ｔｒａｎｓｍｉｓｓｉｏｎ　Ｌｉｃｅｎｓｉｎｇ　Ａｄｍｉｎｉｓｔｒａｔｏｒ、ＬＬＣ）と呼ばれる管理者の管理の下でＤＴＣＰ規格に準拠した機器を相互接続し、その間で暗号認証通信を行っている。その仕組みの概要は次の通りである。

（１）送信機器および受信機器は、それぞれＤＴＬＡから配布された秘密鍵と証明書を備えている。この秘密鍵と証明書の配布はＤＴＬＡとの契約に基づいて各機器に配布される。

【０００７】

（２）送信機器と受信機器は、上記秘密鍵を用いて相互認証する。また、送信機器は、著作権保護が必要となるコンテンツを、認証により共有した鍵で暗号化して送信する。なお、鍵の共有方法はディフィーヘルマン（ＤＨ）鍵共有方法（例えば非特許文献４）をベースにして楕円曲線暗号上にＤＴＣＰ規格で独自に規定されたものである。

【０００８】

ところで、上記ＤＴＣＰコンテンツ保護の仕組みを無線通信の世界まで拡張することを考えた場合、ＩＥＥＥ１３９４のような有線バスと異なり、盗聴やなりすましなどの攻撃が容易であることが懸念される。例えば近くを通りかかった受信機器がＤＴＬＡから配布された秘密鍵を持ってさえいれば、他人の機器が許可無く勝手に接続する危険がある。このことは著作権保護の観点から言って問題である。また、その送信機器を保有する個人がどのようなコンテンツに興味があるのかが暴露する可能性もあり、プライバシー保護の点でも問題がある。

【０００９】

この問題を解決する１つの方法として、無線のセキュリティ機能、例えばＩＥＥＥ８０２．１１ｂで決められているＷＥＰ（Ｗｉｒｅｄ　Ｅｑｕｉｖａｌｅｎｔ　Ｐｒｉｖａｃｙ、例えば非特許文献５）を、上記認証に加えて使用することが考えられる。ユーザはパスワードを予めアクセスポイントに設定し、同じパスワードを機器側に入力しないと接続できない。つまり、パスワードを知らない他人が勝手に接続する危険はなくなる。具体的にはパスワードを用いて、チャレンジデータに対するレスポンスを生成し、これにより認証を行う。さらに、パスワ

ードを用いて通信データのＭＡＣ層での暗号化を行っている。

【００１０】

【非特許文献１】

岡本龍明、山本博資、”現代暗号”、産業図書（１９９７年）、１５５ページ～１５６ページ

【００１１】

【非特許文献２】

American National Standards Institute, American National Standard for Financial Services, ANSX9.57: Public Key Cryptography For the Financial Industry: Certificate Management, 1997.

【００１２】

【非特許文献３】

ＤＴＣＰ　ＳｐｅｃｉｆｉｃａｔｉｏｎのＷｈｉｔｅ　ｐａｐｅｒ　＜ＵＲＬ：　HYPERLINK "http://www.dtcp.com/spec.html" http://www.dtcp.com/spec.html＞

【００１３】

【非特許文献４】

池野信一、小山謙二、「現代暗号理論」、電子通信学会、１７５ページ～１７７ページ

【００１４】

【非特許文献５】

ＷＥＰ暗号化の基礎と実践＜ＵＲＬ：　HYPERLINK "http://www.atmarkit.co.jp/fwin2k/operation/wirelesswep/wirelesswep01.html" http://www.atmarkit.co.jp/fwin2k/operation/wirelesswep/wirelesswep01.html＞

【００１５】

【発明が解決しようとする課題】

上記述べたＤＴＣＰにＷＥＰを組み合わせた方法では、アクセスポイントのＷＥＰをＯＮにする／しないの選択はユーザ任せである。そのためプライバシーの問題はユーザの責任なのでしかたがないが、コンテンツ著作権保護の観点からは

問題である。また、認証部分ではＤＴＣＰの認証とＷＥＰの認証の双方が個別に必要であり、送信機器と受信機器の間のトランザクションが多くなる。さらに、ＤＴＣＰはアプリケーション層でコンテンツの暗号化を行い、さらにＷＥＰではＭＡＣ層での通信データの暗号化を行うため、送信機器および受信機器においてもその負荷は大きい。２重で暗号化するのも無駄である。以上述べたとおり、実装上の観点から課題がある。

【００１６】

本発明では、パスワード認証をＤＴＣＰのような機器認証に組み合わせることにより、コンテンツ著作権保護の課題を解決し、さらに実装上も負荷にならない方法を実現する。

【００１７】

【課題を解決するための手段】

上記課題を解決するために、請求項１における機器認証システムは、第１のネットワークに接続しているサーバにより第２のネットワークに接続している機器を認証する機器認証システムであって、前記サーバは、チャレンジデータを作成し、前記機器へ送信するチャレンジ送信手段と、署名データを受信する署名受信手段と、前記署名データが、前記チャレンジデータと前記サーバに予め設定されている第１のパスワードデータに基づく第１の署名対象データに対する正しい署名であるか否かを検証する署名検証手段を備え、前記機器は、前記チャレンジデータを受信するチャレンジ受信手段と、前記チャレンジデータと、前記機器に予め設定されている第２のパスワードデータに基づく第２の署名対象データを作成する署名対象データ作成手段と、前記第２の署名対象データに対する前記署名データを作成する署名作成手段と、前記署名データを送信する署名送信手段を備える。

【００１８】

請求項２における機器認証システムは、請求項１における前記第２のパスワードデータが、外部から入力されることを特徴とする。

請求項３における機器認証システムは、請求項１の前記機器は、さらに外部より入力された第３のパスワードデータを前記第２のパスワードデータに登録する

パスワード登録手段を備えることを特徴とする。

【００１９】

請求項４における機器認証システムは、請求項３における前記機器は、さらにネットワークを介して前記第３のパスワードデータを受信するパスワード受信手段と、前記第３のパスワードデータが送信されたパスワード送信元が前記第２のネットワークに接続しているか否かを判定するパスワード送信元判定手段を備え、

前記パスワード登録手段は、前記パスワード送信元が前記第２のネットワークに接続していると判定された場合のみに、前記第３のパスワードデータを前記第２のパスワードデータに登録することを特徴とする。

【００２０】

請求項５における機器認証システムは、請求項３における前記機器は、さらに前記第３のパスワードデータの長さを計測し、前記第３のパスワードデータの長さが予め与えられた値以上であるか否かを判定するデータ長判定部を備え、前記パスワード登録手段は、前記第３のパスワードデータの長さが予め与えられた値以上である場合に、前記第３のパスワードデータを前記第２のパスワードデータに登録することを特徴とする。

【００２１】

請求項６における機器認証システムは、請求項１から請求項４のいずれかの１項における前記サーバは、さらに前記第２のネットワークが前記第１のネットワークと同一であることを判定するネットワーク判定手段を備え、前記署名検証手段は、前記判定が肯定的である場合、前記署名データが前記チャレンジデータと前記サーバに予め設定されている第４のパスワードデータに基づく第３の署名対象データに対する正しい署名であるか否かを検証し、否定的である場合、前記前記署名データが前記チャレンジデータと前記サーバに予め設定されている第５のパスワードデータに基づく第４の署名対象データに対する正しい署名であるか否かを検証することを特徴とする。

【００２２】

請求項７における機器認証システムは、請求項１から請求項６のいずれか１項

における前記署名生成手段及び前記署名検証手段で使用する署名方法は公開鍵署名方法であることを特徴とする。

請求項８における機器認証システムは、請求項１から請求項６のいずれか１項における前記署名生成手段及び前記署名検証手段で使用する署名方法は鍵付ハッシュ関数を利用することを特徴とする。

【００２３】

請求項９における機器認証装置は、チャレンジデータを作成し、前記機器へ送信するチャレンジ送信部と、署名データを受信する署名受信部と、前記署名データが、前記チャレンジデータと予め設定されている第１のパスワードデータに基づく第１の署名対象データに対する正しい署名であるか否かを検証する署名検証手段を備える。

【００２４】

請求項１０における機器認証装置は、請求項９にさらに前記機器が接続している第２のネットワークが前記機器認証装置が接続している第１のネットワークと同一であることを判定するネットワーク判定手段を備え、前記署名検証手段は、前記判定が肯定的である場合、前記前記署名データが前記チャレンジデータと前記サーバに予め設定されている第４のパスワードデータに基づく第３の署名対象データに対する正しい署名であるか否かを検証し、否定的である場合、前記前記署名データが前記チャレンジデータと前記サーバに予め設定されている第５のパスワードデータに基づく第４の署名対象データに対する正しい署名であるか否かを検証することを特徴とする。

【００２５】

請求項１１における機器認証方法は、第１のネットワークに接続しているサーバにより第２のネットワークに接続している機器を認証する機器認証方法であって、前記サーバにより、チャレンジデータを作成し、前記機器へ送信するチャレンジ送信ステップと、前記機器により、前記チャレンジデータを受信するチャレンジ受信ステップと、前記機器により、前記チャレンジデータと、前記機器に予め設定されている第２のパスワードデータに基づく第２の署名対象データを作成する署名対象データ作成ステップと、前記機器により、前記第２の署名対象デー

タに対する署名データを作成する署名作成ステップと、前記機器により、前記署名データを送信する署名送信ステップと、前記サーバにより、署名データを受信する署名受信ステップと、前記サーバにより、前記署名データが、前記チャレンジデータと前記サーバに予め設定されている第１のパスワードデータに基づく第１の署名対象データに対する正しい署名であるか否かを検証する署名検証ステップを含むことを特徴とする。

【００２６】

請求項１２における機器認証方法は、請求項１１にさらに、前記機器により、外部より入力された第３のパスワードデータを前記第２のパスワードデータに登録するパスワード登録ステップを含むことを特徴とする。

請求項１３における機器認証方法は、請求項１１にさらに、前記機器により、ネットワークを介して前記第３のパスワードデータを受信するパスワード受信ステップと、前記機器により、前記第３のパスワードデータが送信されたパスワード送信元が前記第２のネットワークに接続しているか否かを判定するパスワード送信元判定ステップを含み、前記パスワード登録ステップは、前記機器により、前記パスワード送信元が前記第２のネットワークに接続していると判定された場合のみに、前記第３のパスワードデータを前記第２のパスワードデータに登録することを特徴とする。

【００２７】

請求項１４における機器認証方法は、請求項１１から請求項１３にさらに、前記サーバにより、前記第２のネットワークが前記第１のネットワークと同一であることを判定するネットワーク判定ステップを含み、前記署名検証ステップは、前記サーバにより、前記判定が肯定的である場合、前記前記署名データが前記チャレンジデータと前記サーバに予め設定されている第４のパスワードデータに基づく第３の署名対象データに対する正しい署名であるか否かを検証し、否定的である場合、前記前記署名データが前記チャレンジデータと前記サーバに予め設定されている第５のパスワードデータに基づく第４の署名対象データに対する正しい署名であるか否かを検証することを特徴とする。

【００２８】

請求項１５における記録媒体は、第１のネットワークに接続しているサーバにより第２のネットワークに接続している機器を認証する処理をコンピュータに実行させるプログラムを記録したコンピュータ読取可能な記録媒体であって、前記サーバにより、チャレンジデータを作成し、前記機器へ送信するチャレンジ送信ステップと、前記機器により、前記チャレンジデータを受信するチャレンジ受信ステップと、前記機器により、前記チャレンジデータと、前記機器に予め設定されている第２のパスワードデータに基づく第２の署名対象データを作成する署名対象データ作成ステップと、前記機器により、前記第２の署名対象データに対する署名データを作成する署名作成ステップと、前記機器により、前記署名データを送信する署名送信ステップと、前記サーバにより、署名データを受信する署名受信ステップと、前記サーバにより、前記署名データが、前記チャレンジデータと前記サーバに予め設定されている第１のパスワードデータに基づく第１の署名対象データに対する正しい署名であるか否かを検証する署名検証ステップとをコンピュータに実行させることを特徴とする。

【００２９】

請求項１６における記録媒体は、請求項１５にさらに、前記機器により、外部より入力された第３のパスワードデータを前記第２のパスワードデータに登録するパスワード登録ステップをコンピュータに実行させることを特徴とする。

請求項１７における記録媒体は、請求項１６にさらに、前記機器により、ネットワークを介して前記第３のパスワードデータを受信するパスワード受信ステップと、前記機器により、前記第３のパスワードデータが送信されたパスワード送信元が前記第２のネットワークに接続しているか否かを判定するパスワード送信元判定ステップをコンピュータに実行させ、前記パスワード登録ステップは、前記機器により、前記パスワード送信元が前記第２のネットワークに接続していると判定された場合のみに、前記第３のパスワードデータを前記第２のパスワードデータに登録することを特徴とする。

【００３０】

請求項１８における記録媒体は、請求項１５から１７にさらに、前記サーバにより、前記第２のネットワークが前記第１のネットワークと同一であることを判

定するネットワーク判定ステップをコンピュータに実行させ、前記署名検証ステップは、前記サーバにより、前記判定が肯定的である場合、前記前記署名データが前記チャレンジデータと前記サーバに予め設定されている第４のパスワードデータに基づく第３の署名対象データに対する正しい署名であるか否かを検証し、否定的である場合、前記前記署名データが前記チャレンジデータと前記サーバに予め設定されている第５のパスワードデータに基づく第４の署名対象データに対する正しい署名であるか否かを検証することを特徴とする。

【００３１】

【発明の実施の形態】

［実施の形態１］

〔実施の形態１の構成〕

図１は、実施の形態１における、サーバ機器１００とクライアント機器１０１の内部構成を示している。以降、サーバ機器１００を単にサーバ、クライアント機器１０１を単にクライアントとも呼ぶ。

【００３２】

サーバ機器１００は、公開鍵暗号系における公開鍵に信頼できる第３者機関（ＣＡ：Ｃｅｒｔｉｆｉｃａｔｉｏｎ　Ａｕｔｈｏｒｉｔｙ　と呼ぶ）の署名が付与された公開鍵証明書を格納する公開鍵証明書格納部１０３と、前記公開鍵に対応する秘密鍵を格納する秘密鍵格納部１０２と、公開鍵暗号の各種処理（署名生成／検証など）を実行する公開鍵暗号処理部１０４と、登録したパスワードをクライアント機器１０１固有の識別子と対応付けて格納するパスワード記録部１０５と、クライアント機器１０１からの応答を用いてクライアント機器１０１が正しい機器であり、さらにパスワードが正しいことを認証する認証部１０６と、クライアント機器１０１との間で通信を行う入出力部１０７からなる。

【００３３】

一方、クライアント機器１０１は、公開鍵暗号系における公開鍵にＣＡの署名が付与された公開鍵証明書を格納する公開鍵証明書格納部１０８と、前記公開鍵に対応する秘密鍵を格納する秘密鍵格納部１０９と、公開鍵暗号の各種処理（署名生成／検証など）を実行する公開鍵暗号処理部１１０と、クライアント機器１

０１固有の識別子を格納する識別子格納部１１１と、ユーザのパスワードを入力を受け付けるパスワード入力部１１２と、サーバ機器１００との間で通信を行う入出力部１１３を備える。

【００３４】

ここで、少なくとも、サーバ機器１００およびクライアント機器１０１における秘密鍵格納部１０２、１０９、サーバ機器１００におけるパスワード記録部１０５は、例えば耐タンパ領域に格納されて、外部に漏れることなく内部で厳重に管理されるものとする。

[実施の形態１のパスワードと機器認証フロー]

図２は、図１におけるサーバ機器１００が、クライアント機器１０１の機器認証およびそれに入力されたパスワードの認証を行う際の動作フローを示している。以下、その詳細について説明する。なお、この動作フローはＤＴＣＰの機器認証にパスワード認証機能を追加しつつ、トランザクションの数および、サーバ機器１００とクライアント機器１０１における計算量は増加しない。

【００３５】

Ｓ２００：ユーザはクライアント機器１０１にパスワードＰＷを入力する。具体的には、クライアント機器１０１におけるパスワード入力部１１２は、ユーザからパスワードＰＷを受け付ける。

Ｓ２０１：クライアント機器１０１はサーバ機器１００に対し、公開鍵暗号処理部１１０で生成した乱数ｒｂと、識別子格納部１１１内に格納されている自身の機器識別子であるＩＤｂと、公開鍵証明書格納部１０８内に格納されている証明書Ｃｅｒｔｂを添えて、認証の要求を行う。

【００３６】

Ｓ２０２：サーバ機器１００はクライアント機器１０１の証明書の正しさを確認する。ＤＴＣＰでは証明書には楕円曲線暗号の署名方法であるＥＣ－ＤＳＡを用いたＣＡの署名が含まれている。この署名をＣＡの公開鍵を用いて検証する。

Ｓ２０３：サーバ機器１００は、公開鍵暗号処理部１０４で生成した乱数ｒａと、公開鍵証明書格納部１０３内に格納されている証明書Ｃｅｒｔａをクライアント機器１０１に送付する。

【００３７】

Ｓ２０４：クライアント機器１０１は公開鍵暗号処理部１１０において、サーバ機器１００の証明書Ｃｅｒｔａの正しさを確認する。

Ｓ２０５、Ｓ２０６：サーバ機器１００およびクライアント機器１０１それぞれにおいて、楕円曲線暗号のＤＨ鍵共有方法であるＥＣ－ＤＨを用いた初期値Ｘａ、Ｘｂを計算する。

【００３８】

Ｓ２０７：サーバ機器１００の公開鍵暗号処理部１０４は、乱数ｒｂをチャレンジデータとして、これに対応した署名応答［Ａ］を生成し、前記Ｘａとともに、クライアント機器１０１に送付する。署名応答は例えば、ｒｂとＸａを連結した情報に対してサーバの秘密鍵を用いて生成する。

Ｓ２０８：クライアント機器１０１の公開鍵暗号処理部１１０は、乱数ｒａをチャレンジデータとし、Ｓ２００で入力したＰＷを用いて署名応答［Ｂ］を生成し、前記Ｘｂとともに、サーバ機器１００に送付する。署名応答は例えば、ｒａとＸｂおよび、ＰＷを連結した情報に対してクライアント機器１０１の秘密鍵を用いて生成する。

【００３９】

Ｓ２０９：サーバ機器１００はクライアント機器１０１の機器識別子ＩＤｂに対応したＰＷを、パスワード記録部１０５から検索し、選択する。そしてクライアント機器１０１から送られた署名応答［Ｂ］を、選択したＰＷを用いて認証する。具体的にはｒａ、ＸｂとＰＷを連結した情報、およびクライアント機器１０１の公開鍵を用いて、クライアント機器１０１の署名応答が正しいことを公開鍵暗号処理部１０４にて確認する。ここで認証が合わない場合は、ＰＷあるいはクライアント機器１０１が正しいものではないと判断し、認証手続きを中止する。

【００４０】

Ｓ２１０：クライアント機器１０１はサーバ機器１００の署名応答［Ａ］を同様に認証する。具体的にはｒｂとＸａを連結した情報、およびサーバ機器１００の公開鍵を用いて、サーバの機器１００の署名応答［Ａ］が正しいことを公開鍵暗号処理部１１０にて認証する。この認証が合わない場合は、サーバ機器１００

が正しいものではないと判断し、認証手続きを中止する。

【００４１】

Ｓ２１１、Ｓ２１２：サーバ機器１００およびクライアント機器１０１はそれぞれ、ＥＣ－ＤＨの初期値を用いて、共通の認証鍵を計算する。

なお、このあとＤＴＣＰでは、サーバ機器１００からクライアント機器１０１に暗号化したコンテンツを配布してクライアント機器１０１においてこれを共通の認証鍵を用いて復号する。

【００４２】

なお、実施の形態１では機器間の認証は双方向、ＰＷの認証は片側（サーバ機器１００がクライアント機器１０１のＰＷを認証）であったが、これに限るものではなく、機器間の認証が片側、あるいはＰＷの認証は双方であっても良い。ＰＷの認証で双方向にするとクライアント機器１０１が以前に自身がＰＷを登録したサーバ機器１００であるかを確認することができる。

【００４３】

［実施の形態２］

実施の形態２では、実施の形態１におけるサーバ機器１００のパスワード記録部１０５にユーザのパスワードを登録する機能を追加する。パスワードの認証は実施の形態１と同じである。

〔実施の形態２の構成〕

図３は、実施の形態２における、サーバ機器１００とクライアント機器１０１の内部構成を示している。

【００４４】

サーバ機器１００は、実施の形態１におけるサーバ機器１００に、パスワード入力部３００と、入力されたパスワードが妥当であるかをチェックするパスワードチェック部３０１と、さらにクライアント機器１０１と近くにあることを認証する近接認証部３０２を追加している。

一方、クライアント機器１０１は、実施の形態１におけるクライアント機器１０１に、サーバ機器１００と近くにあることを証明する近接証明部３０３を追加している。サーバ機器１００およびクライアント機器１０１のその他の構成要素

に関しては、図１と同じであるため、ここでは説明を省略する。

【００４５】

[実施の形態２のパスワード登録時動作]

実施の形態２におけるパスワードの登録には２通りある。１つはサーバ機器１００に直接入力する場合であり、もう１つは近接のクライアント機器１０１からのリモート入力の場合である。

サーバ機器１００に直接入力する場合、入力されたパスワードはパスワードチェック部３０１において、妥当性をチェックしてからパスワード記録部１０５に記録される。妥当性のチェックでは、例えばパスワードの長さが十分であるかどうか、また辞書にある単語ではないか、またアルファベットだけではなく、数字や記号などの情報が含まれているかなどを確認する。

【００４６】

一方、リモート入力の場合、サーバ機器１００とクライアント機器１０１の間で公開鍵暗号を用いた認証と鍵共有を行い、さらにサーバ機器１００とクライアント機器１０１が近くにあるかどうかを確認することにより、クライアント機器１０１から入力されたパスワードがサーバ機器１００に登録される。クラアント機器１０１からサーバ機器１００に伝送されるパスワードは前記鍵共有した鍵を用いて暗号化してもよい。サーバ機器１００とクライアント機器１０１が近くにあるかどうかの確認は、例えば次のような方法で行うとよい。

【００４７】

・ＩＰパケットのヘッダにあるＴＴＬ（Ｔｉｍｅ　Ｔｏ　Ｌｉｖｅ）フィールドを用いる。ＴＴＬはルータを越えるごとにデクリメントされるものである。例えばクラアント機器１０１の近接証明部３０３からある決められたＴＴＬ値でサーバ機器１００にパケットを送信し、サーバ機器１００に到着したときのＴＴＬ値との差分で、いくつルータを越えたのかを近接認証部３０２で調べることができる。この差分値が小さければ、サーバ機器１００とクライアント機器１０１が近くにあると判断することができる。

【００４８】

・サーバ機器１００の近接認証部３０２からクライアント機器１０１にＰｉｎ

ｇパケットを送信し、クライアント機器１０１の近接証明部３０３からの応答が返ってくるまでの時間をサーバ機器１００の近接認証部３０２で測る。この値が小さければ、サーバ機器１００とクライアント機器１０１が近くにあると判断することができる。

【００４９】

これにより、家庭内のクライアント機器１０１からのパスワード登録だけを受け付ける。

［実施の形態３］

実施の形態３では、サーバ機器１００とクライアント機器１０１が近くにある場合と遠くにある場合で、有効となるパスワードを変更することを可能にする。クライアント機器１０１を家庭内で使用する場合は、簡略したパスワードを使用することによりユーザ利便性を確保し、リモートで使用する場合は長いパスワードを要求することにより、セキュリティを高めることが可能になる。

【００５０】

〔実施の形態３の動作〕

実施の形態３の動作を、実施の形態２と同様の図３を用いて説明する。

パスワード記録部１０５には、家庭内で使用する場合のパスワードとリモートで使用する場合のパスワードを記録しておく。

サーバ機器１００は、クライアント機器１０１の機器認証する際に、近接認証部３０２および近接証明部３０３を用いて、クライアント機器１０１が近くにあるのか遠くにあるのかを確認する。この方法としては、前述した実施の形態１と同様のＴＴＬやＰｉｎｇを用いるとよい。そして、その結果に応じてサーバ機器１００はパスワード記録部１０５より、対応するパスワードを選択してパスワード認証時に使用する。パスワード認証は実施の形態１に従う。

【００５１】

なお、実施の形態３においては、家庭内とリモートの２種類のパスワードを使い分ける方法を述べたが、これを複数種類備えても良い。例えばＴＴＬ値が５以下なら第１のパスワード、１０以下なら第２のパスワード、１０より大きいなら第３のパスワードといった具合である。これにより、例えば家庭内なら短いパス

ワードで利便性を向上し、（間のルータ数が少ない）専用線で接続されているオフィスとの間ではある程度の長さを確保したパスワードを利用し、（間のルータ数が多い）海外等の離れたところから利用する場合は、高度のセキュリティを備えたパスワードを利用することが可能となる。

【００５２】

なお、実施の形態１、２、３においては、ＩＤに対応したパスワードを複数設けてもよい。もし１つのパスワードを忘れても覚えているパスワードを用いてサーバ機器１００と認証できる。また、登録できるＩＤとパスワードを複数設けても良い。さらに、ＩＤに対応して使用できるコンテンツを選択しても良い。例えば、家族のそれぞれで利用できるコンテンツを分けることができる。

【００５３】

また、実施の形態１、２、３におけるパスワード入力部は、一般的にはユーザがアルファベットや数字などをキーボードを用いて入力するが、携帯電話やリモコンのようなボタンを用いて入力しても良い。また、毎回は入力しなくてもよい。

また手で入力する替わりに、ＩＣカードやセキュアメモリカードを用いても良い。

【００５４】

また指紋や虹彩などのバイオメトリックス情報を用いても良い。なお、バイオメトリックス情報は、入力時の誤りあるいは生体情報の多少の変動がありうる。この場合は、クライアント機器１０１においてディジタルデータであるパスワードを予め記録し、バイオメトリックスを用いて個人認証を行い、その結果本人であることが認証できた場合にのみ、クライアント機器１０１に記録しているパスワードを使用してパスワード認証を行っても良い。例えば実施の形態３では、リモート環境では、バイオメトリックス情報のみをＰＷとして使用可能とするといった使い方もできる。これにより、よりリモート環境でのセキュリティを高めることができる。

【００５５】

また、上記実施の形態１、２、３では、公開鍵暗号ベースのＰＷ認証と機器認

証を説明したが、使用する暗号の種類は問わない。共通鍵暗号であっても、あるいは鍵を用いたハッシュ関数を用いても構わない。

【００５６】

【発明の効果】

以上のように、請求項１に示した機器認証システムでは、機器認証だけでなく、機器に入力されたパスワードの認証を、そのトランザクションや計算量を増加せずに行うことができる。このことにより、勝手に接続されるというコンテンツ著作権保護の課題を解決する。

【００５７】

また、請求項４ではサーバと機器の間が近いのか離れているのかを判定する手段を加えることにより、リモートでのパスワードの登録を可能とする。

また、請求項６では請求項４と同様にサーバと機器の間が近いのか離れているのかを判定して、必要なパスワードを使い分ける。このことにより、例えば家庭内では簡易なパスワードを用いて利便性を確保し、リモート環境では長く複雑なパスワード、あるいはバイオメトリックス情報を用いて安全性を向上するといった使い方が可能となる。

【図面の簡単な説明】

【図１】

実施の形態１におけるサーバ機器とクライアント機器の内部構成図

【図２】

実施の形態１のサーバとクライアント間の機器認証およびパスワード認証の動作フロー

【図３】

実施の形態２におけるサーバ機器とクライアント機器の内部構成図

【符号の説明】

１００　サーバ機器

１０１　クライアント機器

１０２、１０９　秘密鍵格納部

１０３、１０８　公開鍵証明書格納部

１０４、１１０　公開鍵暗号処理部

１０５　パスワード記録部

１０６　認証部

１０７、１１３　入出力部

１１２、３００　パスワード入力部

１１１　識別子格納部

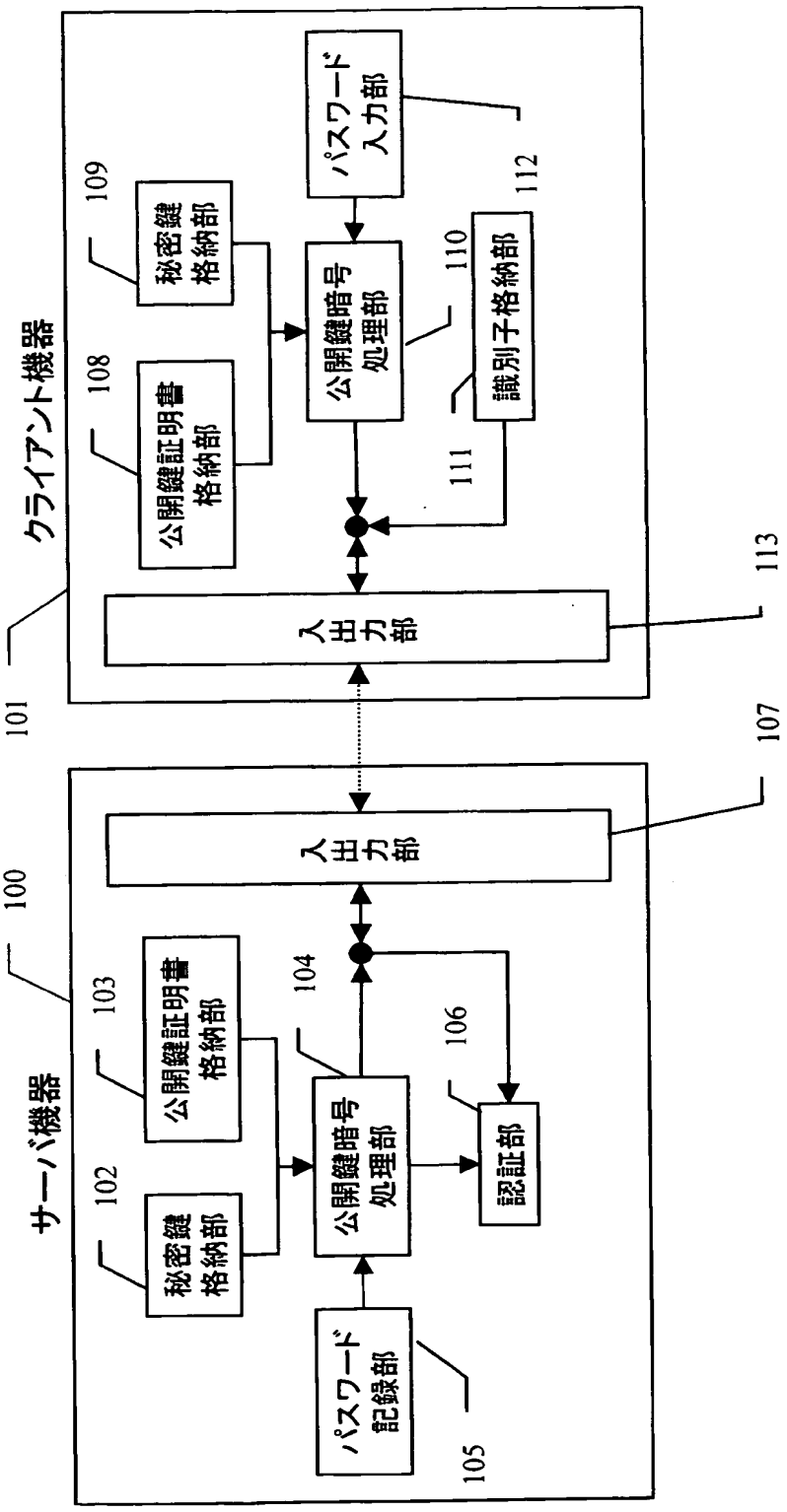
３０１　パスワードチェック部

３０２　近接認証部

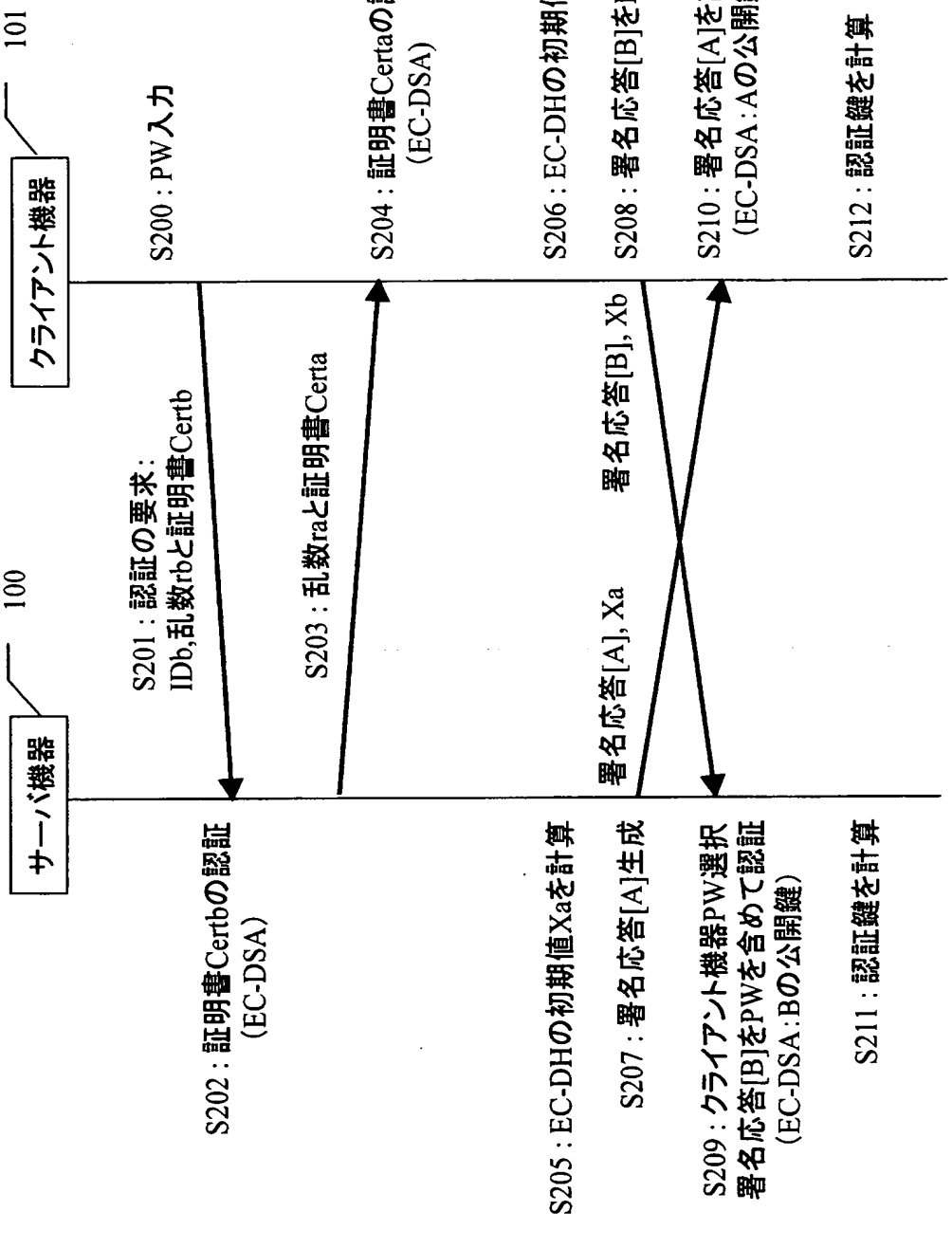
３０３　近接証明部

【書類名】　図面

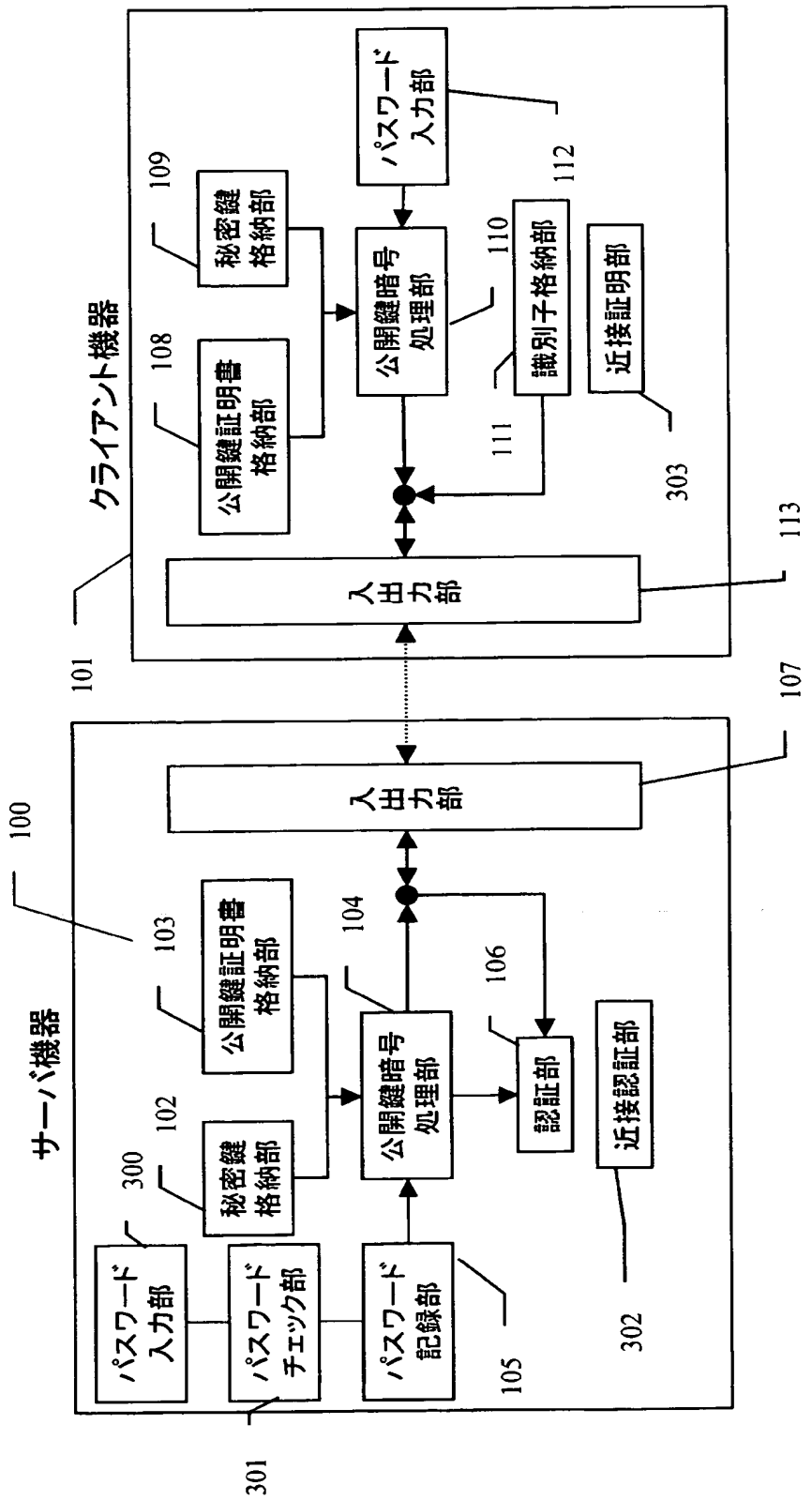
【図１】


クライアント機器
101
秘密鍵格納部
109
公開鍵証明書格納部
108
パスワード入力部
112
公開鍵暗号処理部
110
識別子格納部
111
入出力部
113
107
サーバ機器
100
入出力部
公開鍵証明書格納部
103
104
秘密鍵格納部
102
公開鍵暗号処理部
106
認証部
パスワード記録部
105

【図２】


サーバ機器
100
クライアント機器
101
S200 : PW入力
S201 : 認証の要求 :
IDb,乱数rbと証明書Certb
S202 : 証明書Certbの認証
(EC-DSA)
S203 : 乱数raと証明書Certa
S204 : 証明書Certaの認証
(EC-DSA)
S205 : EC-DHの初期値Xaを計算
S206 : EC-DHの初期値Xbを計算
S207 : 署名応答[A]生成
署名応答[A], Xa
署名応答[B], Xb
S208 : 署名応答[B]をPWを含めて生成
S209 : クライアント機器PW選択
署名応答[B]をPWを含めて認証
(EC-DSA : Bの公開鍵)
S210 : 署名応答[A]を認証
(EC-DSA : Aの公開鍵)
S211 : 認証鍵を計算
S212 : 認証鍵を計算

【図３】


クライアント機器
サーバ機器
入出力部
秘密鍵格納部
公開鍵証明書格納部
パスワード入力部
公開鍵暗号処理部
識別子格納部
近接証明部
パスワードチェック部
パスワード記録部
認証部
近接認証部
100
101
102
103
104
105
106
107
108
109
110
111
112
113
300
301
302
303

【書類名】要約書

【要約】

【課題】　コンテンツ保護の仕組みを無線通信の世界まで拡張したときに、コンテンツ保持者の許可がない機器が、勝手にサーバ機器に接続することを、実装上負荷をかけずに、防ぐことを目的とする。

【解決方法】　機器に入力されたパスワードを含めた署名を、チャレンジデータに対応したレスポンスとする。サーバ機器側は登録されているパスワードを含めてこれを認証することにより、トランザクションや計算量を増やさずに機器認証とパスワード認証を双方とも実現する。

【選択図】図１

特願２００３－１０９２６４

出　願　人　履　歴　情　報

識別番号　［０００００５８２１］

１．変更年月日　１９９０年　８月２８日
［変更理由］　新規登録
住　所　大阪府門真市大字門真１００６番地
氏　名　松下電器産業株式会社